Papua New Guinea

Cybercrime legislation

Table of contents

Version 25 July 2022

[reference to the provisions of the Budapest Convention]

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

State:	
Signature of the Budapest Convention:	N/A
Ratification/accession:	N/A

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Chapter I – Use of terms	
Article 1 – "Computer system", "computer data", "service provider", "traffic data": For the purposes of this Convention: a "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data; b "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function; c "service provider" means: i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and ii any other entity that processes or stores computer data on behalf of such communication service or users of such service; d "traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service	Cybercrime Code Act, 2016 **PART I. - PRELIMINARY.** **Division 1. - Compliance with Constitutional Requirements.** **2. Interpretation** (…) "**computer"** means an electronic, magnetic, optical, electrochemical, or other data processing device, or a group of such interconnected or related devices, performing logical, arithmetic, storage and display functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device or group of such interconnected or related devices, but does not include an automated typewriter or typesetter, or a portable hand held calculator or other similar device which is non-programmable or which does not contain any data storage facility; "**computer program**" means data representing a set of instructions or statements that, when executed in a computer or other electronic device, causes the computer or electronic device to perform a function; (…) "**data**" means any representation of facts, concepts, information (being either text, audio, video, audiovisual or images) machine readable code or instructions, in a form suitable for processing in an electronic system or device, including a program suitable to cause an electronic system or device to perform a function; "**data traffic**" means any electronic data relating to a communication by means of an electronic system or device, generated by an electronic system or device that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service; (…)

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	"**ict service provider**" means a person who provides content, applications or network services or a combination of such services, including, but not limited to, those identified in Schedule 1 and includes their employees, servants, agents or assignees; (…)
Chapter II – Measures to be taken at the national level	
Section 1 – Substantive criminal law	
Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems	
Article 2 – Illegal access Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.	**Cybercrime Code Act, 2016** **PART III. - OFFENCES AND PENALTIES.** **Division 1. - Offences Related to the Integrity of Data and Electronic Systems or Devices.** **6. Unauthorised access or hacking.** (1) A person who, intentionally and without lawful excuse or justification, or in excess of a lawful excuse or justification, accesses or gains entry without authorisation, to the whole or any part of a protected or non-public electronic system or device, or data, is guilty of a misdemeanour. Penalty: Imprisonment for a term not exceeding five years or a fine not exceeding K7,000.00, or both. (2) Where the offence in Subsection (1) results in damage or loss to the whole or any part of an electronic system or device, or data, the offender is guilty of a crime. Penalty: Imprisonment for a term not exceeding 15 years or a fine not exceeding K25,000.00, or both.
Article 3 – Illegal interception Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be	**Cybercrime Code Act, 2016** **PART III. - OFFENCES AND PENALTIES.** **Division 1. - Offences Related to the Integrity of Data and Electronic Systems or Devices.** **7. Illegal interception**

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
committed with dishonest intent, or in relation to a computer system that is connected to another computer system.	(1) A person who, intentionally and without lawful excuse or justification, or in excess of a lawful excuse or justification, intercepts by technical or other means - (a) any non-public transmission to, from or within an electronic system or device; or (b) electromagnetic emissions from an electronic system or device, not intended for him, is guilty of a crime. Penalty: (a) A fine not exceeding K50,000.00 or imprisonment for a term not exceeding 15 years, or both; and (b) In the case of a body corporate, a fine not exceeding K500,000.00. (2) Where the offence under Subsection (1) is committed against State or Military transmissions, or transmissions of other sensitive data, the offender is guilty of a crime. Penalty: (a) In the case of a natural person, a fine not exceeding K100,000.00 or imprisonment for a term not exceeding 25 years, or both; and (b) In the case of a body corporate, a fine not exceeding K1,000,000.00.
Article 4 – Data interference 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right. 2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.	**Cybercrime Code Act, 2016** **PART III. - OFFENCES AND PENALTIES.** **Division 1. - Offences Related to the Integrity of Data and Electronic Systems or Devices.** **8. Data interference** A person who, intentionally and without lawful excuse or justification, or in excess of a lawful excuse or justification or recklessly - (a) damages or deteriorates data; or (b) deletes data; or (c) alters data; or (d) renders data meaningless, useless or ineffective; or (e) obstructs, interrupts or interferes with the lawful processing of data; or (f) obstructs, interrupts or interferes with any person in their lawful use of data; or

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(g) denies access to data to any person authorised to access it, is guilty of a crime. Penalty: (a) In the case of a natural person, a fine not exceeding K20,000.00 or imprisonment for a term not exceeding 10 years, or both; and (b) In the case of a body corporate, a fine not exceeding K100,000.00.
Article 5 – System interference Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data	**Cybercrime Code Act, 2016** **PART III. - OFFENCES AND PENALTIES.** **Division 1. - Offences Related to the Integrity of Data and Electronic Systems or Devices.** **9. System interference** (1) A person, who intentionally and without lawful excuse or justification, or in excess of a lawful excuse or justification, or recklessly - (a) hinders or interferes with the functioning of an electronic system or device; or (b) hinders or interferes with a person's lawful use or operation of an electronic system or device, is guilty of a misdemeanour. Penalty: (a) In the case of a natural person, a fine not exceeding K10,000.00 or imprisonment for a term not exceeding 10 years, or both; and (b) In the case of a body corporate, a fine not exceeding K100,000.00. (2) Where the offence is committed against an electronic system or device that is exclusively for the use or operation of critical infrastructure, or in the case where such electronic system or device is not exclusively for the use or operation of critical infrastructure, but is otherwise used in connection with the operation of critical infrastructure, and such conduct - (a) affects the use of critical infrastructure; or (b) impacts the operation of critical infrastructure, the offender is guilty of a crime. Penalty:

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(a) In the case of a natural person, a fine not exceeding K100,000.00 or imprisonment for a term not exceeding 25 years, or both; and (b) In the case of a body corporate, a fine not exceeding K1,000,000.00 and K25,000.00 for each subsequent day the critical infrastructure remains inoperable.
Article 6 – Misuse of devices 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right: a the production, sale, procurement for use, import, distribution or otherwise making available of: i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5; ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and b the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches. 2 This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system. 3 Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.	**Cybercrime Code Act, 2016** **PART III. - OFFENCES AND PENALTIES.** **Division 2. - Computer Related Offences.** **16. Illegal devices** (1) A person who, intentionally and without lawful excuse or justification, or in excess of a lawful excuse or justification, designs, produces, sells, procures for use, imports, exports, distributes or otherwise makes available - (a) an electronic system or device, or thing that is designed or adapted; or (b) a password, access code or similar data by which the whole or any part of an electronic system or device, or thing is capable of being accessed, for the purpose of committing an offence defined by other provisions of Part III of this Act, is guilty of a crime. Penalty: (a) In the case of a natural person, a fine not exceeding 1 25,000.00 or imprisonment for a term not exceeding 15 years or, both; and (b) In the case of a body corporate, a fine not exceeding K100,000.00. (2) It is a defence to a charge under this section where the design, production, sale, procurement for use, import, distribution or otherwise making available, or possession of devices referred to in Subsection (1), is for authorised testing or protection of an electronic system or device, or for law enforcement purposes. (3) Whether an illegal device referred to in Subsection (1) is for authorised testing, protection of an electronic system or device, or law enforcement purposes, is a question of fact.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Title 2 – Computer-related offences	
Article 7 – Computer-related forgery Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.	**Cybercrime Code Act, 2016** **PART III. - OFFENCES AND PENALTIES.** **Division 2. - Computer Related Offences.** **13. Electronic forgery** (1) A person who, intentionally and without lawful excuse or justification, or in excess of a lawful excuse or justification - (a) inputs, alters, deletes, or suppresses electronic data; or (b) otherwise interferes with the functioning of an electronic system or device, for the purpose of creating or generating inauthentic data that it may be considered or acted upon for lawful purposes as if it were authentic, regardless of whether the data is directly readable or intelligible, is guilty of a crime. Penalty: (a) In the case of a natural person, a fine not exceeding K100,000.00 or imprisonment for a term not exceeding 25 years, or both; and (b) In the case of a body corporate, a fine not exceeding K1,000,000.00. (2) A person who, intentionally and without lawful excuse or justification, or in excess of a lawful excuse or justification, conspires with another person to commit, or attempts to commit an offence under this section, is guilty of a crime. Penalty: (a) In the case of a natural person, a fine not exceeding K15,000.00 or imprisonment for a term not exceeding 15 years, or both; and (b) In the case of a body corporate, a fine not exceeding K500,000.00.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Article 8 – Computer-related fraud Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by: a any input, alteration, deletion or suppression of computer data; b any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.	**Cybercrime Code Act, 2016** **PART III. - OFFENCES AND PENALTIES.** **Division 2. - Computer Related Offences.** **12. Electronic fraud** (1) A person who, intentionally and without lawful excuse or justification, or in excess of a lawful excuse or justification - (a) inputs, alters, deletes, or suppresses electronic data; or (b) otherwise interferes with the functioning of an electronic system or device, for the purpose of deceiving or depriving another person of their property for his own gain or that of another person, is guilty of a crime. Penalty: (a) In the case of a natural person, a fine not exceeding K100,000.00 or imprisonment for a term not exceeding 25 years, or both; and (b) In the case of a body corporate, a fine not exceeding KI,000,000.00. (2) A person who, without lawful excuse or justification, or in excess of a lawful excuse or justification, conspires with another person to commit, or attempts to commit an offence under this section, is guilty of a crime. Penalty: (a) In the case of a natural person, a fine not exceeding 1(25,000.00 or imprisonment for a term not exceeding 15 years, or both; and (b) In the case of a body corporate, a fine not exceeding K500.000.00.
Title 3 – Content-related offences	
Article 9 – Offences related to child pornography 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: a producing child pornography for the purpose of its distribution through a computer system; b offering or making available child pornography through a computer system; c distributing or transmitting child pornography through a computer system;	**Cybercrime Code Act, 2016** **PART I. - PRELIMINARY.** **Division 1. - Compliance with Constitutional Requirements.** **2. Interpretation** **"child"** means, for the purposes of this Act, a person under the age of 18 years; (…) "**pornography"** means - (a) any photographic, film, video or other visual representation -

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
d procuring child pornography through a computer system for oneself or for another person; e possessing child pornography in a computer system or on a computer-data storage medium. 2 For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts: a a minor engaged in sexually explicit conduct; b a person appearing to be a minor engaged in sexually explicit conduct; c realistic images representing a minor engaged in sexually explicit conduct 3 For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years. 4 Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.	(i)that shows a person who is, or who is depicted as, engaged in sexual activity; or (ii) which characteristics is the depiction of any part of the body of a person for or connoting a sexual purpose; or (b) any audio representation of a person who is, or is represented as being, engaged in a sexual activity; or (c) any written material, visual, audio or audiovisual representation that advocates, counsels or encourages sexual activity, irrespective of how or through what medium the representation has been produced, transmitted or conveyed and, without prejudice to the generality of the foregoing, includes any representation produced by or from computer graphics or other electronic or mechanical means; or (d) a representation of sexual activity or sexual engagement with animals; **PART III. - OFFENCES AND PENALTIES** **Division 3. - Content Related Offences.** **18. Child pornography** (1) A person who, intentionally and without lawful excuse or justification, or in excess of a lawful excuse or justification, uses an electronic system or device to commit any of the offences prescribed under Sections 229R, 229S and 229T of the Criminal Code Act (Chapter 262), is guilty of a crime. Penalty: (a) In the case of a natural person, a fine not exceeding K100,000.00 or imprisonment for a term not exceeding 25 years, or both; and (b) In the case of a body corporate, a fine not exceeding K1,000,000.00. (2) A person who, intentionally and without lawful excuse or justification, or in excess of a lawful excuse or justification, uses an electronic system or device to access child pornography, whether or not for the purpose of downloading or transmitting it either to himself or another person, or, for the purpose of giving effect to or facilitating the commission of any of the offences in Subsection (1), is guilty of a crime. Penalty:

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(a) In the case of a natural person, a fine not exceeding K100,000.00 or imprisonment for a term not exceeding 25 years, or both; and (b) In the case of a body corporate, a fine not exceeding K1,000,000.00. (3) It is a defence to a charge for an offence under this section if the child pornography was for a bona fide law enforcement purpose or for the benefit of the public. (4) Whether the doing of an act referred to in this section is for the benefit of the public, is a question of fact. (5) For the purposes of this section, if child pornography is stored for a bona fide law enforcement purpose, all traces, copies, or storage of such pornographic material shall be removed, deleted or otherwise destroyed once it is no longer lawfully required.
Title 4 – Offences related to infringements of copyright and related rights	
Article 10 – Offences related to infringements of copyright and related rights 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system. 2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms	**Cybercrime Code Act, 2016** **PART III. - OFFENCES AND PENALTIES** **Division 4. - Other Offences.** **28. Online copyright infringement** A person who, intentionally and without lawful excuse or justification, or in excess of a lawful excuse or justification, or recklessly, uses an electronic system or device, and knowingly and repeatedly - (a) infringes; or (b) authorises the infringement of; or (c) facilitates or enables the infringement of, a right protected under the Copyright and Neighbouring Rights Act 2000 or any other laws relating to copyright, is guilty of a crime. Penalty: (a) In the case of a natural person - (i) imprisonment for a term not exceeding 15 years; or (ii) a fine not exceeding K100,000.00; or

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system. 3 A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.	(iii) prohibition from accessing and using ICTs or electronic system or devices for the term of imprisonment imposed plus an additional two years; or (iv) all or any of Subparagraphs (i), (ii) or (iii); and (b) In the case of a body corporate, a fine not exceeding K1,000,000.00. **29. Online trademark infringement** A person who, intentionally and without lawful excuse or justification, or in excess of a lawful excuse or justification, or recklessly, uses an electronic system or device, and knowingly or repeatedly - (a) sells; or (b) exposes for sale, goods or services to which a forgery of a registered trademark is falsely applied in contravention of the Trademarks Act (Chapter 385), or any other laws relating to trademarks, is guilty of a crime. Penalty: (a) In the case of a natural person - (i) imprisonment for a term not exceeding 15 years; or (ii) a fine not exceeding K100,000.00; or (iii) prohibition from accessing and using ICTs or electronic system or devices for the term of imprisonment imposed plus an additional two years; or (iv) all or any of Subparagraphs (i), (ii) or (iii); and (b) In the case of a body corporate, a fine not exceeding K1,000,000.00. **30. Patent and industrial designs infringement** A person who, intentionally and without lawful excuse or justification, or in excess of a lawful excuse or justification, or recklessly, uses an electronic system or device, and knowingly or repeatedly commits an act or omission which contravenes the Patents and Industrial Designs Act 2000 or any other law relating to patents and industrial designs, is guilty of a crime. Penalty: (a) In the case of a natural person - (i) imprisonment for a term not exceeding 15 years; or (ii) a fine not exceeding K100,000.00; or

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(iii) prohibition from accessing and using ICTs or electronic system or devices for the term of imprisonment imposed plus an additional two years; or (iv) all or any of Subparagraphs (i), (ii) or (iii); and (b) In the case of a body corporate, a fine not exceeding K1,000,000.00.
Title 5 – Ancillary liability and sanctions	
Article 11 – Attempt and aiding or abetting 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed. 2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention. 3 Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.	[Attempts, aiding and/or abetting are criminalized when expressively mentioned in the articles above]
Article 12 – Corporate liability 1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on: a a power of representation of the legal person; b an authority to take decisions on behalf of the legal person; c an authority to exercise control within the legal person. 2 In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal	**Cybercrime Code Act, 2016** **PART V. - ICT SERVICE PROVIDERS.** **44. Criminal liability of ICT service providers** (1) An ICT Service Provider which - (a) intentionally or knowingly, and without lawful excuse or justification or in excess of a lawful excuse or justification, monitors the information which they transmit or store on behalf of their users or actively seek facts or circumstances indicating illegal activity by their users; or (b) intentionally or without lawful excuse or justification, or in excess of a lawful excuse or justification, initiates or aides in facilitating the action which results in the commission of an offence under this Act or which results in the contravention of any other law in force in Papua New Guinea; or

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority. 3 Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative. 4 Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.	(c) knowingly or upon knowledge of criminal investigations or proceedings, undertakes or omits to undertake an act, thereby concealing, preventing, or frustrating the criminal investigations or proceedings; or (d) does not comply with an order by the Court requiring it to - (i) assist law enforcement in the prevention, investigation, or prosecution of an offence under this Act or any other law in force in Papua New Guinea; or (ii) terminate or prevent a certain action which would result in the commission or continuation of an offence already committed under this Act or any other law in force in Papua New Guinea; or (e) negligently allows an employee to commit an offence under Paragraph (a), (b), (c) or (d), is guilty of a crime. Penalty: (a) In the case of a natural person, a fine not exceeding K100,000.00 or imprisonment for a term not exceeding 25 years, or both; and (b) In the case of a body corporate, a fine not exceeding K1,000,000.00.
Article 13 – Sanctions and measures 1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 2 through 11 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty. 2 Each Party shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions.	[When applicable, sanctions for legal persons are mentioned in the above-mentioned articles]
Section 2 – Procedural law	
Article 14 – Scope of procedural provisions 1 Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings.	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to: a the criminal offences established in accordance with Articles 2 through 11 of this Convention; b other criminal offences committed by means of a computer system; and c the collection of evidence in electronic form of a criminal offence. 3 a Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20. b Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system: i is being operated for the benefit of a closed group of users, and ii does not employ public communications networks and is not connected with another computer system, whether public or private, that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21	
Article 15 – Conditions and safeguards 1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on	Cybercrime Code Act, 2016 **PART I. - PRELIMINARY.** **Division 1. - Compliance with Constitutional Requirements.** **1. Constitutional requirements** (1) For the purposes of Section 41 of the Organic Law on Provincial Governments and Local-level Governments, it is declared that this law relates to a matter of national interest.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality. 2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, *inter alia,* include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure. 3 To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.	(2) This Act, to the extent that it regulates or restricts a right or freedom referred to in Subdivision III.3.C. (qualified rights) of the Constitution, namely - (a) the right to freedom from arbitrary search and entry conferred by Section 44; and (b) the right to freedom of expression conferred by Section 46; and (c) the right to privacy conferred by Section 49; and (d) the right to freedom of information conferred by Section 51; and (e) the right to freedom of movement conferred by Section 52; and (f) the right to protection from unjust deprivation of property conferred by Section 53, of the Constitution, that is necessary for the purpose of giving effect to the public interest in public safety, public order and public welfare and is reasonably justifiable in a democratic society having proper respect and regard for the rights and dignity of mankind taking into account the National Goals and Directive Principles and Basic Social Obligations, because of the risks cybercrime poses to public safety, public order and public welfare, as well as to the successful social and economic development of Papua New Guinea and its citizens.
Article 16 – Expedited preservation of stored computer data 1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification. 2 Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the	**Cybercrime Code Act, 2016** **PART IV. - PROCEDURE IN SEARCH, EVIDENCE, INVESTIGATION, ETC.** **Division 2. - Preservation of Evidence.** **36. Expedited preservation** (1) Where a member of the Police Force, has reasonable grounds to suspect that - (a) data stored in an electronic system or device, or thing is required for the purpose of an investigation or proceeding; and (b) there is a risk that the data, electronic system or device, or thing may be destroyed or rendered inaccessible, he may, by written notice, require a person in control of the data, electronic system or device, or thing to ensure that the data specified in the notice be preserved for a period of up to 14 days. (2) Subject to Subsection (3), the Magistrate may, upon application by the member of the Police Force, authorise an extension for a further 14 days from the expiry of the initial 14 days.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	(3) An application under Subsection (2) shall be made at anytime within the initial 14 days. (4) A person who fails to comply with a request under Subsection (1) is guilty of an offence. Penalty: (a) In the case or a natural person, a fine not exceeding K10,000.00 or imprisonment for a term not exceeding 12 months, or both; and (b) In the case of a body corporate, a fine not exceeding K100,000.00.
Article 17 – Expedited preservation and partial disclosure of traffic data 1 Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to: a ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and b ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted. 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	**Cybercrime Code Act, 2016** **PART IV. - PROCEDURE IN SEARCH, EVIDENCE, INVESTIGATION, ETC.** **Division 2. - Preservation of Evidence.** **36. Expedited preservation** (1) Where a member of the Police Force, has reasonable grounds to suspect that - (a) data stored in an electronic system or device, or thing is required for the purpose of an investigation or proceeding; and (b) there is a risk that the data, electronic system or device, or thing may be destroyed or rendered inaccessible, he may, by written notice, require a person in control of the data, electronic system or device, or thing to ensure that the data specified in the notice be preserved for a period of up to 14 days. (2) Subject to Subsection (3), the Magistrate may, upon application by the member of the Police Force, authorise an extension for a further 14 days from the expiry of the initial 14 days. (3) An application under Subsection (2) shall be made at anytime within the initial 14 days. (4) A person who fails to comply with a request under Subsection (1) is guilty of an offence. Penalty:

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(a) In the case or a natural person, a fine not exceeding K10,000.00 or imprisonment for a term not exceeding 12 months, or both; and (b) In the case of a body corporate, a fine not exceeding K100,000.00. **37. Partial disclosure** Where the Court is satisfied, on application by a member of the Police Force or the Public Prosecutor, as the case may be, that specified data stored in an electronic system or device, or thing is required for the purpose of an investigation or proceeding, the Court may order such person to disclose sufficient traffic data about a specified communication to identify - (a) the ICT Service Providers involved; and (b) the path through which the communication was transmitted.
Article 18 – Production order 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order: a a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and b a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control. 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15. 3 For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established: a the type of communication service used, the technical provisions taken thereto and the period of service; b the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;	**Cybercrime Code Act, 2016** **PART IV. - PROCEDURE IN SEARCH, EVIDENCE, INVESTIGATION, ETC.** **Division 2. - Preservation of Evidence.** **35. Production orders** Where specified data or a printout is reasonably required for the purposes of an investigation or proceedings, the Court may, on application by a member of the Police Force or the Public Prosecutor, as the case may be, order - (a) a person in control of an electronic system or device, or thing to produce specified data or a printout of such data; or (b) an ICT Service Provider to produce information about persons who subscribe to or use its services.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.	
Article 19 – Search and seizure of stored computer data 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access: a a computer system or part of it and computer data stored therein; and b a computer-data storage medium in which computer data may be stored in its territory. 2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system. 3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to: a seize or similarly secure a computer system or part of it or a computer-data storage medium; b make and retain a copy of those computer data; c maintain the integrity of the relevant stored computer data; d render inaccessible or remove those computer data in the accessed computer system. 4 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2. 5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	**Cybercrime Code Act, 2016** **PART IV. - PROCEDURE IN SEARCH, EVIDENCE, INVESTIGATION, ETC.** **Division I. - Authorised Search and Seizure.** **32. Search** (1) Where a member of the Police Force believes that there are reasonable grounds for suspecting that there is in a private place, a data or thing that may provide evidence of the commission of an offence, he may, under a warrant issued under Subsection (2), enter the private place and - (a) search the private place; or (b) seize any such data or thing. (2) Where it appears to a Magistrate, by information on oath, that there are reasonable grounds for suspecting that there is, in a private place, a data or thing that may provide evidence of the commission of an offence, he may issue a warrant directing a member of the Police Force named in the warrant, or all members of the Police Force to search the private place and to seize any such data or thing and take it before a Magistrate to be dealt with according to law. (3) A warrant under Subsection (2) must be executed by day unless, by the warrant, the Magistrate specifically authorises it to be executed by night. (4) Any data or thing seized under Subsection (2) may be detained by a Magistrate, and when it is no longer required as evidence, it may be destroyed under an order of a Magistrate. **33. Search powers** In addition to the powers under the Search Act (Chapter 341), where a member of the Police Force suspects, on reasonable grounds, that a thing may provide evidence of the commission of an offence, he may, in executing a warrant, exercise the following powers:

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(a) operate the electronic system or device, or direct an occupant of the private place to operate the electronic system or device in order to determine whether it contains data or a thing that could be seized; or (b) operate the electronic system or device, or direct an occupant of the private place to operate the electronic system or device to access data (including data stored on a separate storage device or data not held at the private place) or thing if the member of the Police Force believes, on reasonable grounds, that the data or thing might be data or thing that could be seized; or (c) copy the data or thing that could be seized to a storage device and take the storage device from the place; or (d) copy the data or thing that could be seized in documentary form and seize the produced documents; or (e) move any electronic system or device, or thing, at the place subject of the search, to another place for examination in order to determine whether it contains data that could be seized if - (i) it is significantly more practicable to do so having regard to the task it will take to copy the data and the availability of the technical expertise that will be required to do so; and (ii) there are reasonable grounds to suspect that the electronic system or device, or thing contains data that could be seized; or (f) do anything reasonably necessary to prevent loss, destruction or damage to anything connected with the offence; or (g) use other members of the Police Force or other persons authorised under the warrant as reasonably necessary for the search. **34. Assistance** A member of the Police Force may, upon production of a search warrant obtained under Sections 32 and 33, require a person who is not a suspect of an offence but is in possession or control of an electronic system or device, data or thing that is reasonably required for the purposes of an investigation or proceeding, to enable and assist him, if required, to - (a) access and use an electronic system or device, data or thing; or (b) obtain and copy data; or (c) use an electronic system or device, or thing to make copies; or (d) obtain an output from an electronic system or device, or thing in a format that can be read.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Article 20 – Real-time collection of traffic data 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to: a collect or record through the application of technical means on the territory of that Party, and b compel a service provider, within its existing technical capability: i to collect or record through the application of technical means on the territory of that Party; or ii to co-operate and assist the competent authorities in the collection or recording of, traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system. 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	**Cybercrime Code Act, 2016** **PART IV. - PROCEDURE IN SEARCH, EVIDENCE, INVESTIGATION, ETC.** **Division 3. - Powers of Investigation** **40. Collection of traffic data** Where, on application by a member of the Police Force or the Public Prosecutor, as the case may be, the Court is satisfied upon sworn evidence that traffic data associated with a specified communication is reasonably required for the purposes of an investigation or proceeding, the Court may order a person in control of such data to - (a) collect or record traffic data associated with a specified communication during a specified period; or (b) enable and assist a member of the Police Force to collect or record that data.
Article 21 – Interception of content data 1 Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to: a collect or record through the application of technical means on the territory of that Party, and b compel a service provider, within its existing technical capability: ito collect or record through the application of technical means on the territory of that Party, or	**Cybercrime Code Act, 2016** **PART IV. - PROCEDURE IN SEARCH, EVIDENCE, INVESTIGATION, ETC.** **Division 3. - Powers of Investigation** **39. Authorised interception** Where, on application by a member of the Police Force or the Public Prosecutor, as the case may be, the Court is satisfied upon sworn evidence that there are sufficient grounds to suspect that data or communication is reasonably required for the purposes of an investigation or proceeding, the Court shall - (a) order an ICT Service Provider whose service is available in the country to collect or record through application of technical or other means, to permit or

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
ii to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications in its territory transmitted by means of a computer system. 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	assist a member of the Police Force with the collection or recording of data or communication associated with specified communications transmitted by means of an electronic system or device; or (b) authorise a member of the Police Force to collect or record that data through application of technical or other means.
Section 3 – Jurisdiction	
Article 22 – Jurisdiction 1 Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed: a in its territory; or b on board a ship flying the flag of that Party; or c on board an aircraft registered under the laws of that Party; or d by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State. 2 Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof. 3 Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition. 4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law.	**Cybercrime Code Act, 2016** **PART II. - JURISDICTION.** **3. Application** (1) Unless stated to the contrary, the provisions of the Criminal Code Act (Chapter 262) relating to (a) criminal practice and procedure; and (b) jurisdiction, including Sections 12, 13 and 14; and (c) punishments, including Sections 18 and 19, apply to this Act. (2) The provisions of this Act are in addition to and not in derogation of the Criminal Code Act (Chapter 262) or any other law relating to criminal matters, and where there are any inconsistencies between the provisions of this Act and the Criminal Code Act (Chapter 262) or any other law relating to criminal matters, the provisions of this Act shall apply.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.	
Chapter III – International co-operation	
Article 24 – Extradition 1 a This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 through 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty. b Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply. 2 The criminal offences described in paragraph 1 of this article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them. 3 If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article. 4 Parties that do not make extradition conditional on the existence of a treaty shall recognise the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves. 5 Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition. 6 If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or	**Cybercrime Code Act, 2016** **PART VI. - INTERNATIONAL CO-OPERATION.** **47. Extradition** For the purposes of facilitating matters relating to extradition, the provisions of the Extradition Act 2005 applies. Extradition Act 2005 "Forum country" means a country that is a member of the Pacific Islands Forum; "treaty" includes a convention, protocol, or agreement between 2 or more countries; "treaty country" means a country with which Papua New Guinea has an extradition treaty; 7. EXTRADITION OFFENCE. (1) An offence is an extradition offence if: (a) it is an offence against a law of the requesting country, for which the maximum penalty is death or imprisonment for a period of not less than 12 months; and (b) it is an offence against a law of the requesting country, for which the maximum penalty is death or imprisonment for a period of not less than 12 months; and (c) the conduct that constitutes the offence, if committed in Papua New Guinea, would constitute an offence in Papua New Guinea for which the maximum penalty is death or imprisonment for a period of not less than 12 months. (2) An offence is also an extradition offence if, under an extradition treaty between the requesting country and Papua New Guinea, the conduct that constitutes the offence is required to be treated as an offence for which the surrender of persons is permitted by the country and Papua New Guinea.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as for any other offence of a comparable nature under the law of that Party. 7 a Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the name and address of each authority responsible for making or receiving requests for extradition or provisional arrest in the absence of a treaty. b The Secretary General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party shall ensure	
Article 25 – General principles relating to mutual assistance 1 The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. 2 Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35. 3 Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication. 4 Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the	**Cybercrime Code Act, 2016** **PART VI. - INTERNATIONAL CO-OPERATION.** **46. Mutual assistance** For the purposes of facilitating international co-operation the provisions of the Mutual Assistance in Criminal Matters Act 2005 applies. Mutual Assistance in Criminal Matters Act 2005 3. DEFINITIONS. (1) In this Act unless contrary intention appear – "foreign indictable offence" means an offence against the law of another country that, if the relevant act or omission had occurred in Papua New Guinea, would be an indictable offence; "indictable offence" means an offence against the law of Papua New Guinea: (a) that may be prosecuted on indictment; and (b) for which the maximum penalty is death or a term of imprisonment for at least 1 year;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence. 5 Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.	
Article 26 – Spontaneous information 1 A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter. 2 Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.	
Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements 1 Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.	**Cybercrime Code Act, 2016** **PART VI. - INTERNATIONAL CO-OPERATION.** **46. Mutual assistance** For the purposes of facilitating international co-operation the provisions of the Mutual Assistance in Criminal Matters Act 2005 applies. Mutual Assistance in Criminal Matters Act 2005

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
2 a Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution. b The central authorities shall communicate directly with each other; c Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph; d The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times. 3 Mutual assistance requests under this article shall be executed in accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party. 4 The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or b it considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests. 5 The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities. 6 Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions as it deems necessary. 7 The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. Reasons shall be given for any refusal or postponement of the request. The requested Party shall also	7. REQUEST BY FOREIGN COUNTRIES FOR ASSISTANCE. (1) A request under this Act by a foreign country for international assistance in a criminal matter must be made to the Minister or a person authorised by the Minister to receive requests by foreign countries under this Act. 3. DEFINITIONS. (1) In this Act unless contrary intention appear – "Minister" means the Minister for Justice; 9. REFUSAL OF ASSISTANCE GENERALLY. (1) A request by a foreign country for assistance under this Act must be refused if, in the opinion of the Minister: (a) the request relates to an investigation of, or a proceeding for, a political offence; or (b) there are substantial grounds for believing that the request has been made with a view to prosecuting or punishing a person for a political offence; or (c) there are substantial grounds for believing that the request was made for the purpose of prosecuting, punishing or otherwise causing prejudice to a person on account of the person's race, sex, religion, nationality or political opinions; or (d) the request relates to the prosecution or punishment of a person in respect of an act or omission that if it had occurred in Papua New Guinea, would have constituted an offence under the military law of Papua New Guinea but not also under the ordinary criminal law of Papua New Guinea; or (e) providing the assistance would prejudice the sovereignty, security or national interest of Papua New Guinea; or (f) the request relates to an investigation of, or proceeding for, an offence for which the person concerned: (i) has been acquitted or pardoned by a competent tribunal or authority in the foreign country; or (ii) has undergone the punishment provided by the law of that country of that offence or another offence constituted by the same act or omission as that offence. (2) In this sections: "political offence" has the meaning given in the Extradition Act 2005.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
inform the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly. 8 The requesting Party may request that the requested Party keep confidential the fact of any request made under this chapter as well as its subject, except to the extent necessary for its execution. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed. 9 a In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases, a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party. b Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol). c Where a request is made pursuant to sub-paragraph a. of this article and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so. d Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent authorities of the requesting Party to the competent authorities of the requested Party. e Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, inform the Secretary General of the Council of Europe that, for reasons of efficiency, requests made under this paragraph are to be addressed to its central authority.	10. REFUSAL OF ASSISTANCE – MINISTER'S DISCRETION. A request by a foreign country for assistance under this Act may be refused if, in the opinion of the Minister: (a) the request relates to the prosecution or punishment of a person for an act or omission that would not have constituted and offence against Papua New Guinea law if it had occurred in Papua New Guinea; or (b) the request relates to the prosecution or punishment of a person: (i) for an act or omission that occurred, or is alleged to have occurred, outside the foreign county; and (ii) if a similar act or omission occurring outside Papua New Guinea in similar circumstances would not have constituted an offence against Papua New Guinea law; or (c) the request relates to the prosecution or punishment of a person for an act or omission if the person responsible could no longer be prosecuted because of lapse of time or any other reason if: (i) it had occurred in Papua New Guinea at the same time; and (ii) it had constituted an offence against Papua New Guinea law; or (d) the provision of the assistance could prejudice an investigation or proceeding for a criminal matter in Papua New Guinea; or (e) the provision of assistance would, or would be likely to, prejudice the safety of any person (whether in or outside Papua New Guinea); or (f) the provision of the assistance would result in manifest unfairness or a denial of human rights; or (g) the provision of the assistance would impose an excessive burden on the resources of Papua New Guinea; or (h) it is appropriate, in all the circumstances of the case, that the assistance requested should no be granted. 8. ASSISTANCE MAY BE PROVIDED SUBJECT TO CONDITIONS. Assistance under this Act may be provided to a foreign country subject to any conditions that the Minister determines.
Article 28 – Confidentiality and limitation on use 1 When there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and the requested Parties, the provisions of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation	**Cybercrime Code Act, 2016** **PART VI. - INTERNATIONAL CO-OPERATION.** **46. Mutual assistance** For the purposes of facilitating international co-operation the provisions of the Mutual Assistance in Criminal Matters Act 2005 applies.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof. 2 The requested Party may make the supply of information or material in response to a request dependent on the condition that it is: a kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or b not used for investigations or proceedings other than those stated in the request. 3 If the requesting Party cannot comply with a condition referred to in paragraph 2, it shall promptly inform the other Party, which shall then determine whether the information should nevertheless be provided. When the requesting Party accepts the condition, it shall be bound by it. 4 Any Party that supplies information or material subject to a condition referred to in paragraph 2 may require the other Party to explain, in relation to that condition, the use made of such information or material.	Mutual Assistance in Criminal Matters Act 2005 8. ASSISTANCE MAY BE PROVIDED SUBJECT TO CONDITIONS. Assistance under this Act may be provided to a foreign country subject to any conditions that the Minister determines.
Article 29 – Expedited preservation of stored computer data 1 A Party may request another Party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, located within the territory of that other Party and in respect of which the requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data. 2 A request for preservation made under paragraph 1 shall specify: a the authority seeking the preservation; b the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts; c the stored computer data to be preserved and its relationship to the offence; d any available information identifying the custodian of the stored computer data or the location of the computer system; e the necessity of the preservation; and	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
f that the Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data. 3 Upon receiving the request from another Party, the requested Party shall take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law. For the purposes of responding to a request, dual criminality shall not be required as a condition to providing such preservation. 4 A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of stored data may, in respect of offences other than those established in accordance with Articles 2 through 11 of this Convention, reserve the right to refuse the request for preservation under this article in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled. 5 In addition, a request for preservation may only be refused if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests. 6 Where the requested Party believes that preservation will not ensure the future availability of the data or will threaten the confidentiality of or otherwise prejudice the requesting Party's investigation, it shall promptly so inform the requesting Party, which shall then determine whether the request should nevertheless be executed. 7 Any preservation effected in response to the request referred to in paragraph 1 shall be for a period not less than sixty days, in order to enable the requesting Party to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of such a	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
request, the data shall continue to be preserved pending a decision on that request.	
Article 30 – Expedited disclosure of preserved traffic data 1 Where, in the course of the execution of a request made pursuant to Article 29 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted. 2 Disclosure of traffic data under paragraph 1 may only be withheld if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.	
Article 31 – Mutual assistance regarding accessing of stored computer data 1 A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29. 2 The requested Party shall respond to the request through the application of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this chapter. 3 The request shall be responded to on an expedited basis where: a there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or b the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.	**Cybercrime Code Act, 2016** **PART VI. - INTERNATIONAL CO-OPERATION.** **46. Mutual assistance** For the purposes of facilitating international co-operation the provisions of the Mutual Assistance in Criminal Matters Act 2005 applies. Mutual Assistance in Criminal Matters Act 2005 PART 4. – ASSISTANCE FOR SEARCH AND SEIZURE. 19. REQUEST BY PAPUA NEW GUINEA FOR SEARCH AND SEIZURE. (1) This section applies if: (a) a proceeding or investigation for a criminal matter involving an indictable offence or a serious offence against the law of Papua New Guinea has commenced; and (b) the Minister believes, on reasonable grounds, that a thing relevant to the proceeding or investigation may be located in a foreign country. (2) The Minister may request the appropriate authority of the foreign country –

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(a) to obtain a warrant or other instrument that, under the law of the foreign country, authorises: (i) a search for a thing relevant to the proceeding or investigation; and (ii) the seizure of the thing or any other thing that is or may be relevant to the proceeding or investigation and is found as a result of the search; and (b) to arrange for the thing that has been seized to be sent to Papua New Guinea. (3) A thing may be admissible in evidence in the proceeding or used in the investigation, despite it having been obtained otherwise than in accordance with the request, if it: (a) is relevant to the proceeding or investigation; and (b) has been obtained by the appropriate authority of the foreign country by a process authorised by the law of that country other than the issue (as requested by Papua New Guinea) of warrant or other instrument authorising the seizure of the thing. 20. REQUESTS BY FOREIGN COUNTRIES FOR SEARCH AND SEIZURE. (1) The Minister may direct an authorised officer to apply to a magistrate for a search warrant if: (a) a proceeding for, or investigation of, a criminal matter involving a foreign indictable offence has commenced in a foreign country; and (b) the Minister believers, on reasonable grounds, that a thing relevant to the investigation or proceeding is located in Papua New Guinea. (2) The authorised officer must apply to a magistrate for the issue of a warrant to search land or premises for a thing relevant to the investigation or proceeding. 21. SEARCH WARRANTS. (1) If an application is made under Section 20 for a warrant for a thing relevant to an investigation or proceeding in a foreign country, the magistrate may issue the warrant authorising the authorised officer, with such assistance and by such force as is necessary and reasonable: (a) to enter the land or premises; and (b) to search the land or premises for the thing; and (c) to seize it. (2) The magistrate may issue the warrant only if he or she is satisfied that:

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(a) a proceeding or investigation for criminal matter involving a foreign indictable offence has commenced in the foreign country; and (b) the thing for which the warrant is applied is relevant to the investigation or proceeding; and (c) there are reasonable grounds for issuing the warrant. (3) A warrant issued under this section must include: (a) a statement of the purpose for which the warrant is issued, including a reference to the nature of the relevant offence; and (b) a description of the kind of thing authorised to be seized; and (c) a time at which the warrant ceases to have effect; and (d) a statement that: (i) entry is authorised at any time; or (ii) entry is authorised at times specified in the warrant. (4) If, in the course of searching under a warrant issued under this section for a thing of a kind specified in the warrant, an authorised officer finds another thing, the warrant is taken to authorise the authorised officer to seize the other thing if the officer believes, on reasonable grounds, the other thing: (a) to be relevant to the proceeding or investigation in the foreign country or to provide evidence about the commission of a criminal offence in Papua New Guinea; and (b) to be likely to be concealed, lost or destroyed if it is not seized. 22. AVAILABILITY OF ASSISTANCE AND USE OF FORCE IN EXECUTING A WARRANT. (1) The officer who is executing a search warrant (the executing officer) may obtain such assistance as is necessary and reasonable in the circumstances. (2) The executing officer and any police officer who is assisting in executing the warrant may use such force against persons and things as is necessary and reasonable in the circumstances. (3) A person who is not a police officer and who has been authorised to assist in executing the warrant may use such force against things as is necessary and reasonable in the circumstances.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	23. CUSTODY OF THINGS SEIZED. (1) If an authorised officer seizes a thing under a warrant issued under Section 21, the officer must give the thing to the Commissioner of Police. (2) If a thing is given to the Commissioner of Police under Subsection (1), the Commissioner of Police must: (a) inform the Minister as soon as practicable, that the thing has been received; and (b) arrange for the thing to be kept in safe custody. (3) The Minister may give to the Commissioner of Police a direction in writing about how the thing is to be dealt with, (including a direction that the thing is to be sent to an authority of a foreign country). (4) The Minister must direct an authorised officer to return a thing if: (a) the reason for its seizure no longer exists; or (b) it has been decided that the thing is not to be used in evidence in a foreign country or in relation to a criminal proceeding in Papua New Guinea.
Article 32 – Trans-border access to stored computer data with consent or where publicly available A Party may, without the authorisation of another Party: a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.	
Article 33 – Mutual assistance in the real-time collection of traffic data 1 The Parties shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of a computer system. Subject to the provisions of paragraph 2, this assistance shall be governed by the conditions and procedures provided for under domestic law. 2 Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Article 34 – Mutual assistance regarding the interception of content data The Parties shall provide mutual assistance to each other in the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted under their applicable treaties and domestic laws.	
Article 35 – 24/7 Network 1 Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures: a the provision of technical advice; b the preservation of data pursuant to Articles 29 and 30; c the collection of evidence, the provision of legal information, and locating of suspects. 2 a A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis. b If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis. 3 Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.	
Article 42 – Reservations By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation(s) provided for in Article 4, paragraph 2, Article 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11,	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
paragraph 3, Article 14, paragraph 3, Article 22, paragraph 2, Article 29, paragraph 4, and Article 41, paragraph 1. No other reservation may be made.	

Back to the Table of Contents